C-36-B40
#1

Final Report for Period: 09/2003 - 08/2005
Submitted on: 07/12/2006
Principal Investigator: Potts, Colin .
Award ID: 0344004
Organization: GA Tech Res Corp - GIT
Title:
Policy Modularity: Toward a Science of Socially-Embedded System Design

Project Participants

Senior Personnel

Name: Potts, Colin
Worked for more than 160 Hours: Yes
Contribution to Project:

Post-doc

Graduate Student

Name: Jensen, Carlos
Worked for more than 160 Hours: Yes
Contribution to Project:
Carlos Jensen conducted analysis of Internet Browsers and related technologies to uncover embedded goals and values relating to privacy and security.

Name: Elliott, Jason
Worked for more than 160 Hours: Yes
Contribution to Project:
Jason Elliott performed the preliminary design of iWatch privacy disclosure system human interface.

Undergraduate Student

Name: Bae, Ji
Worked for more than 160 Hours: Yes
Contribution to Project:
Ji Bae implemented iWatch, a browser proxy for disclosing privacy and security issues to users and a crawler that produced a database of Internet site's probably associations on which iWatch's alerts is based.

Technician, Programmer

Other Participant

Research Experience for Undergraduates

Organizational Partners

Other Collaborators or Contacts

Idris Hsi's PhD dissertation (funded through an earlier DARPA contract and subsequent College of Computing teaching assistantships) was an important contribution to this research. His dissertation presents an analysis of the embedded ontological commitments of desktop applications such as Microsoft Office suite components and online games.

Activities and Findings

Research and Education Activities:

(1) Analysis of Internet browsing goals, obstacles and scenarios to disclose privacy values and vulnerabilities.

(2) Systematic development of transitional analysis method (STRAP).

(3) Experiments with novice users to assess usefulness of STRAP with minimal training.

(4) Prototyping of privacy-disclosure tool iWatch. (Continued implementation under separate ITR funding.)

Findings:

(1) Developed and refined method, STRAP, for uncovering privacy values and vulnerabilities from descriptions of existing or envisaged applications. This method was designed as a 'transition' method for use by comparative novices with little expertise in privacy, security or goal-/values-oriented analysis of applications and was explicitly modeled after similar work in the domain of usability by Nielsen and Morch. STRAP has been used in trials on descriptions of web browsing technology. The initial aim was to address privacy and/or security as illustrations of values more generally, but the goals and obstacles are so immediately manifest in the case of privacy, it is such a socially important system attribute, and explorations of privacy cross-fertilize other research in this area funded by NSF, that we decided to focus more exclusively than originally planned on privacy values in particular.

(2) Three experiments that formally evaluate the applicability of STRAP by inexpert, non-professional designers (college students) using expert judgments as benchmarks have demonstrated that STRAP out-performs several methods or checklist-based frameworks developed for the disclosure of privacy and security issues in ubiquitous computing technologies. The direct outcome measures of interest were the number and expert-perceived significance of the privacy vulnerabilities identified by the novice subjects. In addition, a secondary measure of interest was the overlap in identified vulnerabilities and therefore convergence by a small group of evaluators on a defined detection criterion. The experiments compared STRAP with frameworks developed by Bellotti and Hong, Langheinrich, and Patrick and Kenny. Although these were developed with ubiquitous technology in mind, the evaluation was more exhaustive, involving system descriptions that included online consumer e-commerce, meeting management and recording for meeting attendees and non-attendees, and shared online calendar management.

Training and Development:

(1) Carlos Jensen graduated from GA Tech with a Ph.D. in 2005 and is now assistant professor at Oregon State University.

(2) Dr. Jensen spent time during the project as a teaching assistant for courses on Computing, Society and Professionalism, and Human-Computer Interaction. It was in this role that he conducted most of the experimental procedures.

(3) The work by Ji Bae on iWatch was an undergraduate senior design project. He graduated in 2005 and is now enrolled in the M.S. degree in computer science at GA Tech as an employee of NCR Corporation.

Outreach Activities:

For the general public, none under this award.

Journal Publications

Books or Other One-time Publications

Jensen, Carlos, "Designing for Privacy in Interactive Systems", (2005). Thesis, Published
Bibliography: PhD. Dissertation, Georgia Institute of Technology, College of Computing.

Web/Internet Site

Other Specific Products

Contributions

Contributions within Discipline:

Within the broader field of computing, the project has contributed a new, low-cost method for evaluating the privacy implications of envisaged or actual technologies from descriptions of that technology's capabilities. Privacy is often regarded as an aspect of security and requires technical skill and deep technology expertise to assess. This work shows that important understandings of privacy issues can be attained by designers and managers who are not specialists in privacy or security. We envisage such approaches being useful in the design and public scrutiny of privacy-relevant technologies.

Within the more specific subdisciplines of software engineering (and more specifically, requirements engineering), human-centered computing, and security technology, the contributions are as follows:

(a) Requirements engineering: A refinement or specialization of existing research in defining requirements from high-level goals and objectives (i) for ease of use by and communication with non-specialist analysts, and (ii) for specific privacy-related goals.

(b) Human-centered computing: An improvement over existing methods for analysis of systems for usable security/privacy.

(c) Security technology: Development of an approach for identifying specific vulnerabilities at a high-level functional or policy level that can be related to implementation issues. (This relation to implementation was not the focus of the current work and remains to be worked out in detail.)

Contributions to Other Disciplines:

No specific contributions to other disciplines was intended by the project. Recently, after the end of the award, however, Prof. Potts has interacted with several colleagues in the field of philosophy (at the CAiSE PHISE workshop and the European Conference on Philosophy and Computing) and the current work and related work in privacy is likely to lead to future collaborations in the area of disclosive computer ethics.

Contributions to Human Resource Development:

None specifically.

Contributions to Resources for Research and Education:

Other than products reported elsewhere, none.

Contributions Beyond Science and Engineering:

It is too early to speak of informing regulatory policy, since this was an exploratory study. However, the aim is to do so by providing intellectual tools that serve a role in the information environment similar to risk assessments for the physical environment.

Categories for which nothing is reported:

Organizational Partners

Any Journal

Any Web/Internet Site

Any Product